Technical Bulletin

featuring emerging technologies in criminal justice information management

1995 Issue Number 1

Computer Crime: An Overview

By Kelly J. Harris, SEARCH

Businesses have long recognized the benefits of installing computers in the workplace. Computers assist daily operations in myriad ways, fostering efficiency, productivity and timeliness. Legions of individual citizens have also recognized the benefits of technology, taking advantage of the computer's increased affordability and ease of use by installing computers in their homes for word processing, financial management and banking, and desktop publishing. Increasingly, Americans have expanded their interaction with the rest of the world through on-line services that promote communication with the rapidly expanding global community of computer users.

Even those who consider themselves "computer illiterate," however, cannot avoid using the technology. Vehicles, televisions, telephones and other household devices are increasingly equipped with computers. Often, without even realizing it, we access and use computers quite capably on a daily basis by making cellular phone calls, electronically transferring funds, and using debit cards, to name a few.

Indeed, the computer has become a business and household convenience that few individuals will live without. According to *U.S. Industrial Outlook 1994*: "The rest of the 1990s will be a time of significant change in the computer industry, with personal computers finally becoming ubiquitous 'information appliances.' "[1] Computers were found in one home in 100 at the beginning of 1980.[2] Today, more than 31 million homes in the United States are equipped with a personal computer[3] and that number is continuing to expand at an accelerated pace.

There are both benefits and costs associated with technology's growing application in our everyday lives. While computers facilitate efficiency, capability and remote communications, the growing power, versatility, portability and accessibility they offer has also been tapped by a criminal element that exploits the device, and that is responsible for using the technology in a

Bureau of Justice Assistance, SEARCH Explore New Technologies

The SEARCH *Technical Bulletin* is a quarterly publication designed to examine emerging technologies in criminal justice information management. Research and publication of the *Bulletin* is funded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice.

The *Bulletins* identify, describe and assess new and emerging technologies that have existing or potential application in criminal justice information management. They alert practitioners to the existence of technologies which can benefit their management of information.

If you would like to submit an article for publication in the *Technical Bulletin*, please contact SEARCH, The National Consortium for Justice Information and Statistics, at (916) 392-2550.

Publication Funded by
BJA Bureau of Justice Assistance

wide variety of criminal activity.

"The increasing reliance on technology as a foundation of society has resulted in gains in efficiency and capabilities that were unimaginable just a decade ago," said Mr. David J. Roberts, SEARCH Deputy Director. "But there are some very real costs associated with these benefits, one of the most prevalent of which is the ever-expanding potential for criminals to manipulate this reliance on computer technology for their own illicit purposes." Computer crime and its complex, technical nature poses serious implications for law enforcement and the justice community in general.

The *Technical Bulletin* is published by SEARCH, The National Consortium for Justice Information and Statistics, with funding from the Bureau of Justice Assistance, U.S. Department of Justice.

This document was prepared under grant number 95-DD-BX-0017, provided by the Bureau of Justice Assistance, U.S. Department of Justice. The points of view or opinions stated in the document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

SEARCH is located at 7311 Greenhaven Drive, Suite 145, Sacramento, California 95831, (916) 392-2550.

The computer's role in crime

As computer use expands to many different aspects of our lives, so does the potential for the computer to be used illegally. According to Mr. Howard Schmidt, Director, Computer Crime Operations, Office of Special Investigations, U.S. Air Force, "Virtually every crime that a person can commit now has the potential of involving a computer. From drug dealing to computer hacking to child pornography, all types of crimes are being committed via computer." Schmidt adds that computer crime is "information warfare," and computer hackers are particularly dangerous because they can block and/or shutdown urgent information services, such as emergency services.

Mr. Jeff Herig, Discipline Coordinator, Computer Evidence Recovery (CER) Unit, Florida Department of Law Enforcement, finds computer-involved crime that runs the gamut: fraud (document, bank check, driver's license and Medicaid), distribution of child pornography, burglary, theft, narcotics trafficking and homicide.

Computer-related crime generally falls into one of three primary categories, though there may be overlap.[4] Computer crime includes cases in which the computer is the *tool*, the *target*, or is *incidental* to the offense.

The computer as a tool. When the computer is the *tool* in an offense, it is typically used by the criminal to facilitate or enable the illegal activity. Examples in this category include using a computer to create fraudulent or counterfeit documents, to accomplish currency and securities theft, embezzlement, corporate fraud and illegal immigrant and social welfare fraud; to distribute child pornography over computer-based networks; and to facilitate gang- and crime-related networking.

In a recent case where a computer was used as a tool in the crime, SEARCH assisted the Long Beach (California) Police Department with the forensic examination of two seized microcomputers. The computers were allegedly used by a gang involved in a payroll check counterfeiting operation that resulted in the loss of millions of dollars to two major banking institutions. The suspects used computer imaging technology and high-resolution scanners and printers to replicate payroll checks.

In another example, the U.S. Customs Service led an international crackdown on a computerized child pornography network in 1993. Computer users in 17 states and two foreign countries were suspected of transmitting and receiving child pornography on their computers via an overseas computer bulletin board system located in Denmark. In March 1993, SEARCH trained federal agents in computer search and seizure techniques. The agents raided 36 locations and seized and examined computers suspected of containing the child pornography.

The computer is the target. A computer can also be the *target* of criminal activity. In this category, the offender is usually a computer "hacker" who illegally gains access to a

puter Crime" and "The Seizure and Examination of Microcomputers" training courses over the last five years. Other organizations, such as the International Association of Computer Investigative Specialists (IACIS), the Federal Law Enforcement Training Center (FLETC) and the Forensic Association of Computer Technologists (FACT), also report growing requests for training in computer-related crime from law enforcement agencies throughout the country.

At FLETC, where nearly 2,000 students are trained daily, 13 new classes have been added to the Financial Fraud Institute Training Division (one of 10 training divisions) that trains officers in the prevention, detection, investigation and prosecution of financial and computer-related fraud.

Increase in federal, state and local computer crime units. Dedicated units at the federal, state and local levels developed to specifically focus on the problem of computer crime are also evidence of its growing menace. For example, at the federal level, the FBI created the Computer Analysis and Response Team (CART), a specialized forensic team dedicated to examining criminal evidence contained on seized computers. CART operates out of the FBI Crime Laboratory in Washington, D.C., and its team of computer scientists search and extract evidence from computers suspected of use in federal crimes.

Within the U.S. Department of Justice, a Computer Crime Unit has been established to focus specifically on computer crime prosecution.

In 1990, Florida was one of the first states to create a state-level computer crime evidence recovery unit. Mr. Herig proposed establishment of and now heads the unit which has expanded to three regional offices throughout the state. Many other states and localities have followed suit. North Carolina, for example, formed its high tech crime unit to respond to the threat of computer crime in the state's "research triangle," which is known for numerous high tech companies involved in research and development that are prime targets for computer crime. Similarly, the Midwest Electronic Crime Association was formed in Minnesota, which is an alliance of a variety of state, local, public and private agencies dedicated to combating computer crime.

In California, a variety of local agencies have established computer crime investigation and prosecution units and task forces are being established in Santa Clara and Sacramento counties to combat the growing need for interagency cooperation.

High tech crime investigation associations. Another trend at the state and federal level is the formation of high technology crime associations. The High Technology Crime Investigation Association (HTCIA) is one of the most widely recognized international high tech associations with 10 geographic chapters and approximately 1,000 members throughout the U.S.

In 1989, IACIS was formed by federal, state and local law enforcement officers who graduated from the first class in Seized Computers and Data Recovery at the FLETC. According to Mr. Schmidt, former vice president of IACIS, the organization is dedicated to the education and certification of law enforcement officers in the field of computer forensic science. IACIS exists to create and establish procedures to train investigators and certify expert witnesses for the recovery of evidence from computer systems.

Growing body of law. Another indication of computer crime growth is the expanding body of law governing and defining computer crime. Prior to the 1980s, many states prosecuted computer crimes under related, but different legal statutes that did not address computer use, such as fraud, embezzlement, pornography, etc. At the time, there were few laws that focused on computer crime specifically. Today, almost every state has adopted computer crime statutes.[7] (See the next issue of the *Technical Bulletin*, which will examine legal issues surrounding computer crime.)

Meeting the challenge

Law enforcement faces challenges on several fronts when investigating and prosecuting computer crime. Computing has not only significantly altered business procedures, but also the nature of criminal activity and law enforcement efforts to combat the crime. Many of the laws that exist in the "paper world" are not easily transferable to the electronic world. Unique qualifications and training are required for computer crime

investigators, new sets of rules apply for investigating computer-related crime, and, as more cases move through the judicial system, the legal framework is continually changing and adapting to this evolving criminal field.

Training. Investigating computer crime requires techniques unique to those of any other crime investigation. Computer crime cases are fraught with complex technical issues due to the very nature that a computer has been involved in the crime. Investigators require training in computer hardware, software, programming, networks, operating systems, and a whole host of other issues. It is not simply the case that an investigator can present a search warrant, enter the premises, unplug the computer and seize it.

The simple act of switching on a computer might trigger an event that would cause the untrained investigator to lose all evidence on a case. Investigators must be able to assess a computer system before seizing it to ensure that the system has not been "boobytrapped" or programmed to sabotage the investigation. A computer can be rigged to delete all information on the hard disk if a certain procedure is not followed exactly, or a specific password is not entered, when turning on the unit.

"While it is true that computer literacy is not necessarily a prerequisite to using computers, particularly at the user-friendly business level," explains Mr. Fred Cotton, SEARCH Training Services Manager, "law enforcement is at a significant disadvantage in trying to investigate a technology that it does not really understand. Law enforcement, and the criminal justice community as a whole, share common ground with the population who are computer users, but not technologically literate. Criminal investigators, prosecutors and judges need to be cross-trained at an in-depth level on the capabilities and limits of computer technology."

For these reasons, and many others, Mr. Howard Schmidt says law enforcement agencies need to tailor training to meet the demands of a changing society. He says that law enforcement recruiters must look for applicants with different types of qualifications than traditional recruiting. "We need to begin recruiting people with technological skills, or at least basic computer system operation knowledge," he said. "Then we can train them how to investigate."

Conclusion

It is true that law enforcement has a lot to learn with respect to investigating computer crime — as computers and technology continue to advance, this may always be the case. The future of law enforcement efforts in this area, however, is not bleak. There are many federal, state and local organizations across the nation geared specifically toward training law enforcement in the latest investigative techniques for combating computer crime. In addition, more law enforcement agencies are realizing the value and the need for high tech training, and are investing more time and resources in educating law enforcement officers.

Computer crime, however, may never be the top priority for an agency with limited funds. According to Mr. Schmidt, "As long as there is blood running in the streets due to gang-related and other violence problems, there will not be a significant amount of money dedicated to combating computer crime. It will always be a lesser priority."

The next edition of the *Technical Bulletin* will address the major legal issues law enforcement must contend with in conducting a legal search and seizure of a computer system.

Endnotes

[1] *U.S. Industrial Outlook 1994 — Computer Equipment*, 35th Annual Edition, U.S. Department of Commerce/International Trade Administration, January 1995, Section 26, p. 20.

[2] *Dedicated Computer Crime Units*, Thomas J. McEwen, U.S. Department of Justice, National Institute of Justice, Office of Communication and Research Utilization, June 1989.

[3] *U.S. Industrial Outlook 1994 — Computer Equipment*, Section 26, page 17.

[4] This is contrasted by Mr. David L. Carter in his article, "Computer Crime Categories, How Techno-criminals Operate," *FBI Law Enforcement Bulletin*, July 1995, pp. 21-26. Dr. Carter identifies a fourth category of computer crime, "Crimes Associated with the Prevalence of Computers," that asserts the simple growth and presence of computers generates new versions of fairly traditional crimes, such as software piracy and counterfeiting.

[5] *U.S. Industrial Outlook 1994 — Computer Equipment*, Section 26, pages 16-18.

[6] Ibid., Section 26, page 19.

[7] See Bloombecker, Jay Joseph, *Computer Crime Laws*, Clark Boardman Callahan, New York, 1993, for a comprehensive overview of computer crime statutes and issues and a compendium of computer crime statutes at both the federal and state level.

computer or network and commits such crimes as malicious or deceptive data alteration, sabotage of computer software or hardware, program or data theft, and computer virus implantation.

The computer is incidental to the offense. Computer usage may also be *incidental* to an offense, where it is neither an element, nor an instrumentality of the crime. Instead, the computer may contain information about a crime, such as evidence regarding its planning or execution, or information about the victim or related parties, which would aid in the investigation and prosecution.

How bad is it?

Quantifying the severity or pervasiveness of computer crime is still a very difficult task. Until recently, there were no law enforcement reporting requirements for this type of crime, mainly because it was still considered a relatively "new" crime. Only recently, a field was added to the National Incident-Based Reporting System (NIBRS) to gather computer crime statistics — the aggregate-based Uniform Crime Reporting system does not contain such a data field. Consequently, few comprehensive, accurate statistical analyses and studies have been conducted. Those that have attempted to quantify computer crime have come up with such wide-ranging and contradictory statistics that they really tell very little.

To add to the dilemma, major corporations and financial institutions, which are frequently the targets of computer crime, often are reluctant to report the crime, fearing public perception that the institution is weak and has had a breach in security. In addition, the institution seeks to prevent future thefts by withholding details of such offenses.

Computer crime is on the rise. Despite the absence of solid statistics on computer crime, there are a number of factors that indicate computer crime is on the rise. The sheer prevalence of computers in everyday life, law enforcement's growing caseload involving computer crime and the demand for training in this area, the growing number of federal, state and local computer crime investigation units, and the ever-changing body of law addressing computer crime, are strong indicators computer crime is a growing problem.

In addition, major federal agencies involved in computer crime investigation and prosecution, including the Federal Bureau of Investigation (FBI), Customs Service, Secret Service and Department of Justice, all report an increase in computer crime caseloads and for training in proper investigative techniques.

Computer use in the U.S. It is important, initially, to look at the prevalence of computers in our society. According to the *U.S. Industrial Outlook 1994*, personal computer (PC) shipments to the U.S. in 1993 totaled 13.2 million units. The value of the U.S. PC market during the same year was approximately $25 billion. More than 31 million U.S. households owned PCs in 1993, and approximately 67 percent of the small business sector (i.e., 4 million firms with less than 100 employees) had PCs in their firms. It is estimated that during 1993, there were 31 million home-worker households, responsible for purchasing more than two-thirds of the PCs sold to the home market.[5]

Additionally, in the international arena, the world market for PCs totaled $68 billion in 1993, with an active, installed base of 157 million PCs. *U.S. Industrial Outlook* speculated favorable growth for the PC market in 1994, with a 13 percent growth of 16.3 million units.[6]

These figures illustrate that millions of people use computers on a daily basis, and the numbers are growing and will continue to do so rapidly. Computers are becoming an integral aspect of our business and personal lives that are increasingly indispensable. And, as the methods of managing and operating business and personal lives change, so will the methods that criminals use to commit crimes.

Law enforcement demand for training. In addition to studying the widespread use of computers in society, we know that computer crime must be growing by reviewing the experiences of law enforcement agencies throughout the nation. The number of crimes law enforcement officials are asked to investigate that involve computers is rising rapidly, and, as a result, demand for training in this highly-specialized area has increased proportionally.

SEARCH Training Services staff have experienced a steady increase in the demand for "The Investigation of Com-

Resources

SEARCH
7311 Greenhaven Drive, Suite 145
Sacramento, California 95831
(916) 392-2550

Electronic Frontier Foundation
1550 Bryant Street, Suite 725
San Francisco, CA 94117
(415) 436-9333

FBI Academy
Economic and Financial Crime Training Unit
Quantico, Virginia 22135
(703) 640-1156

Florida Assn. of Computer Crime Investigators
NCIS RA Jacksonville
Jacksonville, FL 32212-0058
(904) 772-3334

Forensic Association of Computer Technologists
Iowa DCI Crime Laboratory
Wallace State Building
Des Moines, IA 50319
(515) 281-3666

International Assn. of Computer Investigative Specialists
P.O. Box 2370
Portland, Oregon 97208
(503) 668-4071

High Technology Crime Investigation Assn.
P.O. Box 2046
Walnut, California 91788-2046

National Center for White Collar Crime
Training and Research Institute
11 Commerce Drive, Suite 200
Morgantown, WV 26505
(304) 291-2080

U.S. Customs Service
Department of the Treasury
Office of Enforcement
Smuggling Investigations Division
1301 Constitution Avenue, NW Room 5418
Washington, D.C. 20209
(202) 927-0358

U.S. Department of Justice
Criminal Division, Computer Crime Unit
1001 G. Street, N.W. Suite 200
Washington, D.C. 20001
(202) 514-1026
(202) 616-0307

U.S. Secret Service
Department of the Treasury
Financial Crimes Division
1310 L Street, NW Room 200
Washington, D.C. 20005
(202) 435-7700

Technical Bulletin

featuring emerging technologies in criminal justice information management

James Brantley
Acquisitions
National Criminal Justice
Reference Service
Box 6000
Rockville, MD 20850

SEARCH
The National Consortium for Justice Information and Statistics
7311 Greenhaven Drive, Suite 145 ◦ Sacramento, California 95831
Telephone (916) 392-2550